Privacy & Security Policy Workgroup
Draft Transcript
February 3, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the HIT Policy Committee Privacy and Security Policy Workgroup call this afternoon. There will be an opportunity at the close of the meeting for the public to make comment; meanwhile, I ask the members of the workgroup if you could please remember to identify yourselves when speaking. Let me do a roll call now and see who is on the line. Deven McGraw?

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Paul Tang? Mike Klag?

Mike Klag – John Hopkins Bloomberg School of Public Health - Dean
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Judy Faulkner or Carl Dvorak? John Blair? Paul Egerman? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Uhrig? Dave Wanser?

Dave Wanser – NDIIC – Executive Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Kathleen Connor?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Rachel Block?

Rachel Block – New York eHealth Collaborative – Executive Director
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Loral Stein? Terri Shaw? John Houston? Joyce DuBow? Mike DeCarlo will be dialing in for Justine Handelman, are you on the call Mike?

Mike DeCarlo - BCBS
I am, thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Connie Delaney? Marianna Bledsoe?

Brenda Fran - NIH
Brenda Fran for Marianna Bledsoe.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thanks, Brenda. Peter Basch? Sue McAndrew? Jodi Daniel?

Carl Dvorak – Epic Systems - EVP
And this is Carl Dvorak, I was not on the speaker before but I was on.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, thanks, Carl.

Carl Dvorak – Epic Systems - EVP
I got back in.

Judy Sparrow – Office of the National Coordinator – Executive Director
And Jodi's on and Sarah Wattenberg?

Sarah Wattenberg – ONCHIT – Public Health Advisor
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay.

Joyce DuBow – AARP Public Policy Institute – Associate Director
It's Joyce DuBow.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joyce DuBow, thank you. Anybody else, did I leave anybody off?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
John Houston just joined in.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thanks, John. Okay with that, I'll turn it over to Deven and Rachel.

Deven McGraw – Center for Democracy & Technology - Director
Great, thank you, Judy, thank you very much, and thanks to everyone for so efficiently getting on this call today. We've got an hour and a half to get through what is really a fair amount of material, and I think it'll be a challenge, but I think we're up to it. This is the last scheduled call that we have before the policy committee meeting on February 17th, which is our opportunity to present any recommendations to the

policy committee that we might make with respect to the meaningful use proposed rule; as well as signaling some direction that we're heading in with respect to future policy and standards priority for things that we may feel or maybe not quite ready to be in the rule; or may be out of scope because they weren't necessarily addressed in the first round, but we wanted to put out a flag so that folks know a little bit of where we're headed.

So with that, I've got control of the slides, so I'm going to be moving through them. I want to underscore what are purpose is today, which is to try to come to agreement on recommendations or comments to present to the policy committee on the privacy and security section of the meaningful use notice of proposed rulemaking. And then the second piece of that is to agree on any recommendations that we might want to make at this time that are not necessarily specific to the proposed rule, but instead signal our intent to focus on candidates for priority for either further standards development for example or stage two meaningful use criteria.

So that's what we're really trying to do here on a 90 minute call, and as Judy mentioned, we do need to leave some time at the end for public comment. So let's just jump right in with a very quick review of what's actually in the privacy and security section of the meaningful use proposed rule. And for each meaningful use criteria, there's both an objective to be met, as well as a specific measure that's mostly done through attestation, but is the "proof" that the either eligible provider or hospital has in fact met the objective.

And the objective here is protecting electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. And then the measure is conducting and reviewing a security risk analysis per this is the regulatory site for the risk analysis portion of the security rule, so it's already a requirement in the security rule. And then implementing security updates as necessary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven?

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I was reviewing the NPRM this week for this workgroup and one of the suggestions that I have is that even at the higher level than where you're now, in the definitions of the three stages there's no mention of security and privacy at any stage. And I think we should make some very specific recommendations on some wording on how they can at least get some security and privacy flavor in those definitions themselves.

Deven McGraw – Center for Democracy & Technology - Director
I don't have an objection to that, although, I'll have to go back and look through the meaningful use rule myself. I certainly have recollections and looking at the policy committee materials that it was made fairly specific that all of this was to proceed with appropriate protection for privacy and security.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Deven McGraw – Center for Democracy & Technology - Director
If anyone objects, let me know, but an overarching comment to that regard, it certainly couldn't hurt.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't understand how that doesn't, I mean, the priority that talks about ensuring privacy and security protection for personal health information, I thought was sort of a blanket statement about that, is that not right?

Deven McGraw – Center for Democracy & Technology - Director
Yes, no, I mean I think it's a there. Dixie, can we talk offline about why you think this is missing?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Sure, yes, I had started writing this down, so yes.

Deven McGraw – Center for Democracy & Technology - Director
Okay. Let's leave that to an offline conversation.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Deven?

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
This is Paul Tang, just wanted to let you know, I came in as a non-speaker initially.

Deven McGraw – Center for Democracy & Technology - Director
Okay, yes. I wanted to leave a little bit of time for folks to make sure they got into the right bucket, but unfortunately, we're really pressed today.

Gayle Harrell – Florida – Former State Legislator
Deven, this is Gayle.

Deven McGraw – Center for Democracy & Technology - Director
I'm glad you're on. So did anybody else join us that missed the roll call?

Gayle Harrell – Florida – Former State Legislator
Deven?

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Gayle Harrell – Florida – Former State Legislator
This is Gayle; I was also at the non-speaker to start with.

Deven McGraw – Center for Democracy & Technology - Director

Okay. Alright, great, Gayle.

Jodi Daniel – ONC – Director Office of Policy & Research
And Jodi Daniel is now on.

Deven McGraw – Center for Democracy & Technology - Director
Okay, great, thanks, Jodi, anybody else? Okay, super, alright, so now that we sort of have a level set on what the language is that's in the proposed rule, at least specifically with respect to criteria and objectives, what I've done here in these slides, what we've done is to set out some draft recommendations that are based on discussions that we had on the previous call. So it should look at least somewhat familiar to you all, but we used this time period between calls to try to capture what with the comments that were made and to try to shape them into something that would look like a recommendation that we could then discuss.

What we've got here may clear that for EPs and for those of you who don't know what that means, that's the acronym for eligible professionals. The category of people eligible to receive a financial incentive, so it's physicians and a handful of others, and hospitals who have never, make it clear that if they've never conducted a security risk assessment, which may be the case even though the rule requires it, but the rule only requires it for electronic data. In fact, if they're adopting records for the first time, they may never have actually done one of these. The requirement is that they have to conduct it for their first one.

And so that the option to do reviews should be only for those entities who have recently conducted a security assessment and I posited that we may or may not want to specify a timeline here, that's certainly not something that we discussed in the first call, but I wanted to put that on the table. Therefore, for new adopters of technology, the security assessment would then take place in the first payment year, and then in year two, there would need to be a review, what they would do on an annual basis would just be to review to assess any new threat. And then entities that are in fact significantly upgrading their technology to meet the criteria would then be required to do the new assessment in the first payment year. And then of course, once you've done that full assessment, subsequent years would be reviewing it for new risk.

And then in terms of what types of criteria would trigger a review of security once you've done a full assessment, we might think about tasking ONC, OCR, the standards committee, are there others who would be appropriate to come up with criteria that in fact should trigger a security review. And just to give you a sense of what's coming in case you didn't get a chance to read through these before the meeting, there is a recommendation about providing them with guidance on how to do a security review. And there is a recommendation with respect to clarifying what is meant by implementing security updates as necessary. This is the distinction between software updates versus correcting deficiencies that show up in the security assessment. We had a fair amount of discussion about this on our last call.

So those three recommendations kind of fit together, and I'm going to go back to recommendation number one that we just discussed, but I wanted to give you a flavor of that whole package of recommendations that deals with the security assessment that's already in the rule and is meant to strengthen it and make it more clear.

Gayle Harrell – Florida – Former State Legislator
Deven, this is Gayle.

Deven McGraw – Center for Democracy & Technology - Director
Hello, Gayle.

Gayle Harrell – Florida – Former State Legislator
Hello. Is there a specific requirement that not only do they do the assessment, but they actually implement the changes to deal with the risks that are identified?

Deven McGraw – Center for Democracy & Technology - Director
Yes, well that goes to the question of what is meant in the rule by implement necessary security upgrades. So as you see in the measure, and I just went back on the slide, they're supposed to, not just conduct the assessment or review the assessment, but also to implement security upgrades as necessary. The third recommendation in this package gets to clarifying what that is, but it's definitely part of the measure already.

Gayle Harrell – Florida – Former State Legislator
Because security updates to me says you must install the software.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Gayle Harrell – Florida – Former State Legislator
So unless it's security—

Deven McGraw – Center for Democracy & Technology - Director
Can we hold off on discussing that piece until we get, I want to get some comments specifically on trying, whether it makes sense to clarify when a full-scale review needs to be conducted versus just an upgrade. Because again, in the first payment year and the second payment year, and both of those payment years are part of stage one.

Joyce DuBow – AARP Public Policy Institute – Associate Director
So Deven, isn't the first question—

Deven McGraw – Center for Democracy & Technology - Director
And don't forget to identify yourself.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I'm sorry, it's Joyce. Isn't the first question the one you posed in number one, which asks how recently they conducted it, because that suggests how often it should happen?

Deven McGraw – Center for Democracy & Technology - Director
Right. So here's what I'm positing that if you're a new adopter of electronic technology, your first year should be—

Joyce DuBow – AARP Public Policy Institute – Associate Director
You should demonstrate.

Deven McGraw – Center for Democracy & Technology - Director
--a full security assessment.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Right.

Deven McGraw – Center for Democracy & Technology - Director

But then in subsequent years, you should do a review and maybe there ought to be some specific criteria or event that would naturally trigger a review, such as a major software upgrade done by the vendor, significant changes in rules that need to be accommodated.

I didn't want to suggest that we could come up with an exhaustive list of what those criteria were, but just acknowledging that putting in a recommendation that in fact, that it would be helpful in fact to providers to give them a list of things that could potentially trigger the need for them to review their security assessment.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, I think this might also be in that list of folks to perhaps team for guidance on this.

Deven McGraw – Center for Democracy & Technology - Director
Good idea.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it's important for you to make sure we include the word "risk" here. We're not just talking about a security assessment of looking at what technologies they've implemented, but really a risk assessment.

Deven McGraw – Center for Democracy & Technology - Director
Right, that's fair. And in fact, I should have picked up that language; it's already in the measure.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, it's called risk analysis in the measure.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I think we should, that's exactly what we want them to do.

Deven McGraw – Center for Democracy & Technology - Director
Any other comments on this piece? Alright, well let's move to the second one then. We also recommend that eligible professionals and hospitals be given guidance on how to do one of these. And at the top of the list is if there were guidance to be issued by OCR on what they would look for in a HIPAA security audit, that would be of most help in focusing entities on the critical issues. This was my way of wording the audit program guidance that I don't know exists today, but that John Houston mentioned, would be very helpful. I sensed on the call that folks agreed, so that's top on the list.

Then there's material from CMS, ONC, OCR, and NIST, I remembered NIST on this list, should be made available through multiple channels. I should put the Internet on there, because that's where the security guidance from CMS is already on there, but state HIEs, Medicaid offices, CMS regional offices, regional extension centers, and others.

And then the third piece here is something else that we talked about in the meeting, which is that if you decide to use an external security auditor, which you don't have to do under the security rule today, but if you do one, you should be able to submit the external audit and implementation of any recommended improvements from that audit as proof of meeting the measure. Although, I wrote that down and then I put in another option in brackets, which it would be good for you to have on hand in the event that you in

fact are audited for whether you did this or not; in part because I'm not sure that CMS actually wants you to submit these since most of the meaningful use criteria are done through attestation.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, I think where this is really a security audit is something entirely different from a risk assessment. I think we're mixing apples and oranges here. I think they had it right, that these organizations should be doing a risk assessment where they identify the new vulnerabilities, the new threats, and try to quantify or qualify the risk that they've taken on, that's very different from an audit.

Deven McGraw – Center for Democracy & Technology - Director
I see. But isn't it possible, well, Dixie, unfortunately, we didn't have you on the last call, but isn't it actually possible that some entities, particularly the ones that are larger in size might actually hire—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Not an auditor, they might hire a consultant to help them do a risk assessment. The audit is something different.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I think they call themselves auditors, like URAC for example, Dixie, that do sort of ...

Deven McGraw – Center for Democracy & Technology - Director
And is that Kathleen?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes, I'm sorry, this is Kathleen. I think it's just ... here that they're not auditors like the auditors for your books.

Joyce DuBow – AARP Public Policy Institute – Associate Director
But we don't have any knowledge of whether the audit that's conducted by an external entity that hasn't been deemed officially would be satisfactory.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's not what we want them to do either. We don't want them to just come in and say, "Okay, do you have policies? What are they? What are they?" They were right to begin with. If they've already done a risk assessment, which is required by HIPAA, that's another point. An audit isn't required by HIPAA, a risk assessment is required by HIPAA. But if they've already done it, now that they have their EHR technology, they need to stand back and completely re-do their assessment of their risk.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Okay, I'm going to say again, I think we may want to offline take a look at what entities in the marketplace are using to do their risk assessment, they get consulting groups, some of which are certified or acknowledged by the industry to be best practices who do HIPAA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't care who does it, I'm just saying that we should be consistent with the law of HIPAA and with the language even that the—

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes.

Deven McGraw – Center for Democracy & Technology - Director
Dixie, we can fix the language. What I want to get a sense of, of folks on the call, and just let me take a step back and try to address Joyce's point, which is that while we don't have necessarily a specific accreditation process for an external consulting firm, we also don't have any way of judging the sufficiency of a risk assessment that a provider would do all on her own.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
But CMS—

Deven McGraw – Center for Democracy & Technology - Director
But that's all that's required under HIPAA.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
But Deven, CMS has the right to audit that if it's done by attestation and they present information, CMS can then subsequently audit it.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
But you don't have the same opportunity if somebody external does that and you accept that from a third party, that's all I'm saying. Typically, when you accept the conclusions of a third party, CMS has done something to deem that the standards of the third party are comparable to CMS's standards.

Deven McGraw – Center for Democracy & Technology - Director
Well that's right, but since it's just done through attestation, and again, I think all that we're trying to do here is to acknowledge that in fact, and this is based on the previous call, maybe we don't need to acknowledge this at all. But we had a little bit of discussion on the last call about the options that of course people have to use an external consultant to help them do their risk analysis and whether that could serve as documentation. And the reality is, is that attestation is all that's needed across the board. So maybe we don't need to say anything at all, but the reason why it's listed here is because we did have some discussion about it on our last call and I wanted to put it in a proper context.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't think we need to even address whether they get somebody else, I see what you're talking the audit. What you're trying to address is whether they have a third party re-check, but I think we just have to address that they do a risk assessment and whether they choose to use an external audit of that risk assessment is up to them.

Deven McGraw – Center for Democracy & Technology - Director
Well that's absolutely right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm looking here at the security rule that says, conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI. And that's exactly what we want them to do is to re-do that now that they have EHR technology.

Deven McGraw – Center for Democracy & Technology - Director
Well, and the reality is, Dixie, isn't it the case since the security rule only applies to electronic PHI, that a paper based office that was just transmitting claims electronically might not have ever done one of these.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Very true and probably they haven't.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
... entirely different. It would be like who's coming in the door.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes.

Deven McGraw – Center for Democracy & Technology - Director
Well, right, but they don't, I mean, in the paper world—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
...

Deven McGraw – Center for Democracy & Technology - Director
--they didn't have to.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's right.

Deven McGraw – Center for Democracy & Technology - Director
Alright, we can take that piece out. I don't know that it was, it doesn't really advance the ball much, given that it's an option that's out there already. Let's move on, I suggest we move on to the third one, which is what is meant by implementing security updates as necessary.

And we went back and forth a fair amount on our last call about whether this is just installing security updates that come from the technology vendor or whether this is about implementing, correcting any deficiencies that are, and I'll get rid of the term audit, Dixie, correcting any deficiencies that are identified in the risk assessment.

Now I've also got and we've got more on this later in the slides, but including that the implementing of the updates and addressing "deficiencies" could also include making appropriate and effective use of the new security technical functionalities and standards that are present in the certified EHR technology.

Gayle Harrell – Florida – Former State Legislator
I think that is extremely important that not only they do the assessment, but they implement the changes, both electronic and also perhaps within their normal workflow procedures. It's got to be both, because sometimes it can be workflow and passwords and things of that sort and not just software updates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think that's a really important point that we should make it clear that it includes their security policy and procedures as well, which is what Gayle is talking about really.

Gayle Harrell – Florida – Former State Legislator
Yes, exactly.

Paul Egerman – eScription - CEO
Hello, it's Paul Egerman joining a little bit late.

Deven McGraw – Center for Democracy & Technology – Director
I was just about to ask if you were on the call, Paul.

Paul Egerman – eScription - CEO
Just barely made it.

Deven McGraw – Center for Democracy & Technology - Director
Paul had passed onto me a suggestion to be even more clear about what they ought to be doing with respect to software updates, and so I'm going sieve the floor to him so he can make his point. Paul, are you okay with that?

Paul Egerman – eScription - CEO
Yes. I'm just signing on now, so is the slide up or something?

Deven McGraw – Center for Democracy & Technology - Director
Yes, yes. The slide where it says clarify what is meant by implement security updates as necessary. And where you broke into the discussion, there seems to be general agreement that it should involve both installing the software updates, as well as addressing deficiencies that are identified in the risk assessment. I don't know that we've necessarily closed that conversation, but I know you have a point related to the software upgrade piece.

Paul Egerman – eScription - CEO
Yes. First, the issue is as whether or not the security update meant software updates that come from vendors, so like from these Microsoft updates, or does it mean security updates that come from the security assessment. First, my answer to that is, well let's take both of them. This has to clarify that they're both important things and let's do both.

Then on the software update, we had a discussion in our last meeting where I sort of put forward a fairly aggressive thing saying that everything had to be done within 30 minutes or something and/or in 30 days, and people objected to that. So I've tried to put forward basically a more, I don't know how to describe a more incremental, a more thoughtful approach, simply saying that organizations have to have a written policy that describes how they will promptly implement software upgrades from vendors. And if their policies says that they're going to do delays, if there's interoperability concerns, they have to describe how they're going to either resolve those concerns or possibly work around whatever the security problem is.

And again, my intention there was simply to get organizations to pay attention to these things by having a policy as to what to do with it. At least to do that as a first step.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
In the recommendations that the standards privacy and security workgroup passed over to the policy committee, we did not use the word updates, and I don't recall exactly what the words were. But what we said was once they've done the risk assessment, they should go to their technology and implement those features that were part of the certification that are intended to counter the risk that they've identified.

For example, if they need to, the technology will have the capability to encrypt, but their risk assessment should tell them where they need to encrypt data versus not. And their technology may have the capability to generate an audit trail, but their risk assessment will tell them what information they need to capture in the audit, and how often they need to review the audit and those kind of things. So it's like, take your risk assessment and then decide which features to turn on to counter the risks that you've identified.

Paul Egerman – eScription - CEO
Right. And that's helpful, and to me that's an interpretation. Because all it said in the NPRM was promptly or something like that, implement security updates.

Deven McGraw – Center for Democracy & Technology - Director
Yes. When we had it up ...

Paul Egerman – eScription - CEO
And so some people interpreted that the way you are—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – eScription - CEO
--as be relating to the security assessments.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, yes.

Paul Egerman – eScription - CEO
When I read it, I interpreted it as meaning vendor software updates. And if I remember correctly at the call that we had I wasn't alone, other people also interpreted that comment that way.

Deven McGraw – Center for Democracy & Technology - Director
No, I think they did, but what I think I'm hearing, at least from those of us who have had a chance to talk during this call, that folks are very interested in having both dimensions represented. The software update piece, and Paul, I actually like very much the language you suggest that they've got to deal with them, and let me see, I actually can read it right off of the e-mail that you sent me, because I had hoped to be able to cut and paste it in, but I couldn't get my act together with respect to this, making the technology work.

But it's basically, "The hospital or EP must have a written policy that's described as a process to promptly apply security updates from vendors. And if the updates are not applied within six months of being issued because of interoperability problems with other applications, then the written policy must describe the steps that will be taken to either correct that interoperability problem or avoid the security risk that the updated intended to resolve."

Gayle Harrell – Florida – Former State Legislator
Is six months a rather long period of time? I think that is rather absorbent.

Deven McGraw – Center for Democracy & Technology - Director

I think we'd want those to be acted on promptly. But if you think about the small practice that is in primary care where they're seeing so many patients a day and maybe they don't have a lot of staff, it may be more time than is desirable, but perhaps maybe it's no later than six months.

Paul Egerman – eScription - CEO
...

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes. Deven, I agree with you with the small practice and their resources, but even for the large institutions, some of these things create a significant effort across an enterprise, which has budgetary considerations that have to be planned.

Paul Egerman – eScription - CEO
It's interesting, your comment there, John, I have to tell you my experience with this, is that it's actually a bigger challenge for the large organizations than it is for the small organizations.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes.

Paul Egerman – eScription - CEO
I know that seems a little counter intuitive, but the issue is, you look at large organizations like say Geisinger and you literally have thousands of terminals and there's always an issue of IT priorities and where does this all stand.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
But that's even so much the issue, because my institution is incredibly aggressive about patching and installing security updates, but there are a variety of reasons why they don't get installed, which nothing has to do with the institution itself. And I'll give you a couple of examples. Let's just say we get a Microsoft patch that's considered to have a high severity to the patch, if our vendors don't certify those patches, which many of which will simply don't. We can't install them for fear of malfunctioning of the equipment and some of this equipment is FDA certified equipment. So we can't do it unless the vendor authorizes it, that's the first thing.

Second thing, some of these patches may have a conflict with a revision level of a piece of software that we're running. A good example is for most of our major clinical systems, we don't necessarily put the latest revisions in immediately, we might skip a revision because of the amount of implementation associated with it. So even if we want to put a certain patch into an operating system issue or some other type of layered application patch, we may find that because we're not on the right version of our vendor software, we can't do it, or to get to the right version is something that might be planned 6 to 9, 12-months out.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I agree with John, and I think that this is an area that probably warrants further investigation by experts and maybe ONC can, I don't know what's appropriate here, but this is a big issue about aligning

especially updates for security with devices and the requirements around changing devices. Dixie, I think you've talked about that in the past as well.

Paul Egerman – eScription - CEO
I agree it's a big issue, however, all I'm asking is that organizations have a written policy that describes how they're going to handle it. In other words, that's really all that I'm asking for.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I think that's exactly right. But I also think that they've left a big hole in not, especially since there will be security features in the technology that they can turn on and off.

Deven McGraw – Center for Democracy & Technology - Director
But that's what we're trying to speak to that too, Dixie. We're not just dealing, I mean, the recommendation as it's written doesn't just deal with the software upgrade piece.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, it really does. I was just opening, looking at it in the NPRM and I sort of interpreted it as meaning both implementing the security features and updating software, but they really are talking about what Paul was just talking about, implementing these upgrades.

Deven McGraw – Center for Democracy & Technology - Director
What I meant to say is, I'm sensing from the conversation that's going on in the workgroup is that we would like to recommend that it mean more.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology - Director
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Or unless at the same time. I like Paul's recommendation of making it policy to implement appropriate upgrades rather than just plain implement upgrades. I think he's right on, on that one.

Paul Egerman – eScription - CEO
So to try to respond to some of the concerns I had, I know it's a complicated issue, but all I'm trying to do is ask especially the large organizations to start taking what I would call a thoughtful approach to it, to simply write a policy as to how they're going to handle it.

And the reason again why I think that that's important is that some organizations really have very good policies and they have a good sense of what they're trying to do. but other organizations have almost a belief of, well, if it isn't broken, don't fix it, and don't realize that a security notice means that what they have is broken.

It turns out Deven and I were a call yesterday, there was an emergency room physician there who made the comment that his hospital is currently using Internet Exployer version 4. And when I heard that comment I actually looked up Internet Exployer version 4 and I discovered it was 13 years old, that's like way behind in terms of any kind of security stuff.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

They'll probably never get a virus either, because it's so old.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – eScription - CEO
That's hard to know, but the issue there is again, all I'm saying that this is really aimed at institutions like that is that written policies is to get people to at least start the process of thinking about this. And I'm not proposing, Dixie, that this is the only thing we do, in other words, I want to do both. In other words by both being encourage a written policy on the software upgrade and also the things that you were referring to, to make sure that we promptly and thoughtfully respond to security assessment information.

Gayle Harrell – Florida – Former State Legislator
I also want to address this, because if you're going to have many institutions who are not doing these security upgrades when they become available for whatever reason, you are just going to lose the public big time. And you have to be very careful that people understand that their hospitals and their large institutions and even the primary care docs are doing everything they can to make sure that they are secure.

This is a critical point. When you set long timeframes and you give too many options out there to people not to do it, and you're sitting there on, if you're going to get, we're putting Federal dollars into this and taxpayer money, people are going to expect results.

Paul Egerman – eScription - CEO
Yes, I agree with what you just said, Gayle. The other point I'd make is based on other things going on, the environment is changing. We're asking these institutions to provide patient access to data, which means usually they'll be some sort of patient portal. We're asking them also to be involved with a lot of the interoperability issues, which means sending and receiving data, and so in effect they're opening themselves up a little bit.

Gayle Harrell – Florida – Former State Legislator
Yes, they are, Paul, I agree with you, and that's why it's so important that these securities be in place.

Deven McGraw – Center for Democracy & Technology - Director
Okay, I think I'm sensing, what I want to do is again, because we're short on time, I'm sensing that we're coalescing around some similar thoughts here. I'm going to suggest, because it's already hinted at on this particular slide, the connection between addressing deficiencies and the standards and the functionalities on security that have to be in the certified technology. And I wanted to skip forward a little bit and not in a permanent way, but I'm realizing now that these ideas fit together.

I'm skipping ahead to slide 10, where we've got some recommendations that try to tie those, actually using the functionalities and standards that are in the technology. You'll recall on that previous slide that we just talked about, it suggested that what they ought to do after a security risk assessment is to address any deficiencies, including how they're going to use the new technologies that are in the certified EHR systems or modules that they're purchasing with Federal dollars.

Carl Dvorak – Epic Systems - EVP
One of the observations that I feel that we've seen is that the larger places tend to actually have a chief security officer or a privacy officer designated, and they actually sort of do have policies around many of

these things that are being discussed. But on the smaller practice side that's where they tend not to have anybody.

And I'm wondering if one of the initiatives really ought to be a simplified code of how to do certain things so that we can make practice sustainable for people that don't have the infrastructure of a major health system. And it seems like the trend is for more and more and more complication and more regulation, but I wonder if for those practices we need to do something that would help them sustain and actually accomplish it. They're either going to be—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The other way to slice this one is to make some type of recommendation that as long as a certified EHR is implemented by a certified implementer at a small practice, they supply a set of criteria, that that would then suffice from a security perspective. Because I agree, a small physician practice, they're going to laugh at this stuff, they don't do this. They don't have no sophistication or a desire to do these types of things.

Carl Dvorak – Epic Systems - EVP
Which is a little bit of a concern, because you want them to do some of these things very carefully. And I don't know if you could shift it to a certified implementer, because many things go beyond the scope of the EHR and get into how they deal with office automation and all mentioned Web browsers. But I do think we could come up with or recommend the creation of a simplified code of how to do this sort of thing, having them spend some of its energy on that and validate that it's a reasonable thing for a small or medium office setting.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
There are some very nice guidance's out on HHS were for actually conducting risk assessments, but those could be made even more user friendly, and I agree with you about having NIST take a look at it. The other thing I like about it, those are geared more to small providers and are little vague and they could be ratcheted up for larger providers including ones who have to deal with this very difficult issue around FDA approved medical devices.

And the thing that you could do with this, is that you could also as the technology changes, you would have an opportunity to raise the bar or adjust how the risk assessment was being done. And folks could feel that if they finish this risk assessment that that was something that they could be comfortable that they had the right documentation to handoff if they were audited.

Paul Egerman – eScription - CEO
I just want to remind everyone, we also have another capability to help the small practice, which is the regional extension centers.

Deven McGraw – Center for Democracy & Technology - Director
But I think, yes, I completely agree, but I guess I'm confused, because we had a recommendation about providers getting education about this. So if what you're suggesting, John or Carl, something beyond that?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't see what the big, these are requirements of HIPAA. And yes, I don't care if you're a one person practice, it's not really hard to assign somebody security responsibility. They're supposed to be doing all of this stuff already.

John Blair – Tacanic IPA – President & CEO
Let me ask if practically speaking, you're the one physician practice with maybe a part-time nurse and a receptionist/secretary.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, right, and the receptionist ...

John Blair – Tacanic IPA – President & CEO
... who's going to do that work?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
...

Paul Egerman – eScription - CEO
Let me answer that question, which is probably the best solution for that one physician practice, a solo practitioner, is to have the vendor do it for them. Because if there's that, there will be, if there aren't already vendors who will just say, "We'll take care of this for you."

John Blair – Tacanic IPA – President & CEO
I think that's probably right. I think as this becomes and we understand that it's asked for under HIPAA, but I would agree most of the small practices don't do it, but as it becomes part of meaningful use and there's attestation and audit, they will need to. And as these vendors are claiming that they will get these practices to meaningful use or assist them, that will become part of that assistance.

Paul Egerman – eScription - CEO
Yes, in fact, there's already one vendor at Senna Health that says, "Sign up with us, we'll take care of everything, we'll even guarantee that you'll qualify for meaningful use." I don't know how they do that, but that's what they do. One of the ways they do it is I think they do it through a hosted solution, so that you don't really have to have hardware on site and they just take care of everything for you.

John Blair – Tacanic IPA – President & CEO
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Egerman – eScription - CEO
And that's a very good solution in my opinion for a lot of organizations, not necessarily everybody, but that's probably how a lot of small practices are going to get this stuff done. And it's actually, because there's a lot of stuff that's similar to that, sort of like, I don't know about you, but I never do my own income tax, I have somebody handle it for me.

John Blair – Tacanic IPA – President & CEO
There's still a need for that.

Gayle Harrell – Florida – Former State Legislator
Paul, I'd like to address workflow as well. You've got passwords and you've got people in your office when they get fired or leave or whatever, that you also have to address those kinds of issues in addition to the software issues.

John Blair – Tacanic IPA – President & CEO
Yes, and I agree with that to the point of host and solutions, that won't take care of all that needs to be done at the practice with workflow, but they do train them on the software. They do interact with the practices. And to extend this out, those other educational pieces and support pieces, I think that the vendors will just start to incorporate that into their ongoing training and support, but they're just not focusing on that right now—

Deven McGraw – Center for Democracy & Technology - Director
I think that's right, because John—

John Blair – Tacanic IPA – President & CEO
--because they haven't had to.

Jodi Daniel – ONC – Director Office of Policy & Research
I'm a little concerned about the time and getting ...

Deven McGraw – Center for Democracy & Technology - Director
As am I, because I think we're just reinforcing things we've already said.

Jodi Daniel – ONC – Director Office of Policy & Research
Yes, could we just focus on, I mean, this is really interesting and a helpful discussion, but since we're going to have to deliver on recommendations for these regulations, I'm just ...

Deven McGraw – Center for Democracy & Technology - Director
Thanks, Jodi. So I think the question on the table is, to what extent do we want to be more specific that part of addressing deficiencies ought to include addressing how you're going to utilize the new security features in your certified EHR technology?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Gayle Harrell – Florida – Former State Legislator
Absolutely.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Configure the security capabilities to counter the identified risk.

John Blair – Tacanic IPA – President & CEO
I think there's a misnomer throughout this that the EHR technology, I think it brings a focus on an EHR, but actually you're more significant risk area is the network security, the file access security, what happened if somebody exports the report to excel, those are things that actually go outside the EHR. The EHR certainly has certain elements of it, like passwords, and don't share passwords, etc. But I think there's an odd thing about this in that much of it is environmental in the office how they set things up, how their DSL is wired, do they have a firewall, those sorts of issues go way beyond the EHR technology; even if you outsource the EHR technology, you're still coming in it through the network and likely still having information float through an unprotected zone there if you're not ...

Deven McGraw – Center for Democracy & Technology - Director
Right. So I don't think we mean to say that that's the only thing you need to do, and we can be clear about that. I mean, a risk assessment is a risk assessment that should uncover all the vulnerabilities that

you ought to address. But what I'm suggesting is that one piece of that ought to be considering how you're going to, having policies or a program for utilizing the features that are now in the technology.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I'm very concerned about being prescriptive, I like the outcome. I don't really know that we should be telling them how to do it or that they should be doing x or y, I want to know that they've done it. And I want CMS to be able to determine that they've done it. So if we need criteria for CMS to determine that they have satisfactorily accounted for the risks and have acted on them, that's what I think we want to see, not that they're using the functionalities to do it. Because I want to know what the result is.

Deven McGraw – Center for Democracy & Technology - Director
Joyce, I think you're absolutely right, but I think the reality, I think we have to deal with a couple of realities here. One is that given the volume of providers who are going to be adopting these things for the first time, there isn't really a way for CMS to go into every office and make sure that it's being done and that's true of all the meaningful use criteria quite frankly. But you attest under in a way that you have to defend if you ever get audited.

Joyce DuBow – AARP Public Policy Institute – Associate Director
...

Deven McGraw – Center for Democracy & Technology - Director
What I'm suggesting is, that if you've got new features in your technology that are in fact security protective, but there's no connection right now in meaningful use to actually using them, I'm just suggesting we make that simple connection.

Joyce DuBow – AARP Public Policy Institute – Associate Director
That there be attestation that they are integrating those features into their workflow, is that what your, I mean, is this simply a question of attestation?

Deven McGraw – Center for Democracy & Technology - Director
It's got to be attestation, Joyce, I'm—

Joyce DuBow – AARP Public Policy Institute – Associate Director
Okay, okay, I hear what you're saying.

Deven McGraw – Center for Democracy & Technology - Director
If they're audited I'm not sure what else is possible quite frankly.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Okay, okay. I withdraw my concern.

Deven McGraw – Center for Democracy & Technology - Director
Yes, there's just a limit to what we're able to sort of police on an individual office basis, but I think we'll go very far, way farther than we're today, if we set up some stronger requirements, but then even if they're done through attestation, there's the threat of audit that in addition to I think people are generally honest hangs over folks.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Okay. I withdraw my concern.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
There's value in even forcing them to think about these things.

Deven McGraw – Center for Democracy & Technology - Director
Right, that's right.

Paul Egerman – eScription - CEO
And I do think, Deven, if there were more of a phrasing around EHR technology environment, that the little things are what's going to actually create the compromises like the keystroke loggers that ... get your passwords to an Athena or to another server somewhere and provide other accesses though they were used. I think this inappropriately narrowed down to just the EHR when in fact the real concern is the HIPAA type things with EHR plus that environmental aspect. And I'm not sure whether the environmental aspect is really clarified for people.

Deven McGraw – Center for Democracy & Technology - Director
Yes, I think it's fair to make the point that the risks are not just inherent in the technology.

Joyce DuBow – AARP Public Policy Institute – Associate Director
And that's the point that I've been trying to make.

Deven McGraw – Center for Democracy & Technology - Director
Yes. Well stated to everyone who's been trying to make that point. Alright, well let me get to, this has been a very good call, let me get to something that we started to talk about on the last call and we had some kind of unanswered questions that we wanted to dig into, and that is the question about whether compliance with the HIPAA privacy and security rule ought to be restored as a stage one objective under meaningful use.

And the reason why I'm using the term restored is because it was in the original policy committee metrics that was adopted by the policy committee and then forwarded onto ONC and CMS for their consideration. It did not get into the meaningful use rule, in part because CMS shared with the policy committee in our last meeting, they were concerned about what would trigger something like a suspension or a bar to payment.

Essentially what I've got on this slide is just a rationale for why they ought to consider restoring compliance with federal law as an objective. And then in recommendations 2 through 4, there's a little more detail about how this would get operationalized. So as you'll see in number 2, what I put out here is that eligible professionals in hospitals that essentially have not met the meaningful use privacy and security objectives, if they've received a notice of determination of OCR, that's the Office of Civil Rights that enforces HIPAA, of OCRs intent to impose a civil monetary penalty due to willful neglect of the privacy and security rules. So this is just federal action here and we know that state AGs can enforce the privacy rule, but I specifically not put that in the recommendation because I don't know how it could be operationalized with the state government needing to notify CMS, but obviously we can talk about that.

The criteria then are satisfied when OCR issues a letter closing the investigation, or again because we know there's appellate process here, the final appeal has essentially been adjudicated.

And then if it's a criminal HIPAA investigation, we would apply the same, you're not meeting meaningful use if you're under criminal investigation, but I have phrased that as being criminal investigation of the entity itself and not of a wayward individual within an entity.

Let me just put this all out for you and then we should definitely talk about it. And I have posited that it's not a full bar, it's just a suspension of your payment until it's resolved. The question about whether in fact we want to make it a permanent bar if you get to the point where you have to pay fines or civil monetary penalties, so that's why that's in brackets.

And the one piece of this that I was not able to iron out before the call and that I think might be a contingency on this recommendation is if we only want it to be a suspension of payment until the formal investigation is resolved, does that end up becoming a permanent bar if it doesn't get resolved within the payment year, or is there in fact some way for that payment to sort of be held. I put in escrow, that's probably too technical, a legal term that also involves payment of interest, but I'm not sure we'd necessarily want to use. But the idea here is it's in suspense and not permanently taken off the table.

And again, this is the trigger that Sue McAndrew potentially offered, I wouldn't say she necessarily endorsed it, because it's not OCR. I'm sure she knows that, she doesn't feel that's OCRs job. This is our decision to make with respect to our recommendations, but that's a formal trigger when you get this letter of a notice of intent to pursue civil monetary penalties. And it's at the absolute highest level of a HIPAA civil offense, which is willful neglect, which is already defined in the HIPAA regulations as conscious intentional failure or reckless indifference to the obligation to comply with the provision that's violated.

Paul Egerman – eScription - CEO
Deven, I don't quite understand this second concept of a criminal investigation by for example a state attorney general would that be covered?

Deven McGraw – Center for Democracy & Technology - Director
I'm suggesting that the state piece not be on the table. I actually don't think the state AGs have criminal-investigatory authority, although I've differed with some lawyers on that. I think that their authority to investigate at least under federal law is limited to issuing civil monetary penalties, but even in that case I didn't put it. This is a big step and if I'm out of step with the rest of the workgroup and they want to add the state AG piece, one thing that I did note on these slides is that states could certainly suggest imposing this as a state level Medicaid meaningful use criteria.

Paul Egerman – eScription - CEO
Yes. It troubles me that you would suspend payments just based on an investigation.

Deven McGraw – Center for Democracy & Technology - Director
Well—

Paul Egerman – eScription - CEO
Because you could have, let's say a state attorney general, it's like prosecutorial abuse, who decides to investigate their local university because they get a lot of headlines. But if all you have is a criminal investigation, you could be holding up millions of dollars of money for that institution when they haven't done anything, because they may be found innocent of the investigation.

Deven McGraw – Center for Democracy & Technology - Director
Well right, and so that's why, I did not sense that a permanent bar to funding was something that the workgroup would necessarily endorse. But based on the previous, and again, maybe we're not ready to

go this far, but I sensed from our previous conversation that folks were interested in talking more about this with respect to the most egregious offenses, which in the criminal context is intentional. And again, none of the criminal cases that I'm aware of under HIPAA have ever been brought against an enterprise. They've all been brought against the wayward employee who steals records, and there have been one where a nurse blackmailed somebody. They haven't been levied against an institution, because it's an intentional crime.

And limiting it in the civil case, again to willful neglect, which is a pretty serious HIPAA violation, and triggering it, not at the complaint stage, but at the stage where OCR has received a complaint and in fact thinks there's willful neglect involved and issues an intent to pursue a civil monetary penalty versus informally resolving it. And even then, at least under the main text that I wrote in the recommendation, once it's resolved, whether you're found innocent or not or you've gone through your appeals and you in fact pay a monetary settlement, you then would have met the meaningful use criteria, at least in the way that I first conceptualized this. Although, I think folks may feel differently if and in fact a fine has been paid about whether in fact there ought to be eligibility for dollars. I guess I'm almost recognizing that this is a lot for everyone to consider.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, did you ask the Office of Civil Rights what they were willing to share in terms of who they were investigating, at what point, like do they disclose when they have issued one of these intent to, what is this called, what did you call it?

Deven McGraw – Center for Democracy & Technology - Director
Intent to impose a civil, they have never issued one.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The point, my question really is, what are they willing to disclose? Because I've been in other conversations about this topic and I've been told that in general they don't disclose and are not willing to disclose much about who they're investigating, how it's going, how far they are, or they kind of do all this with the utmost privacy with recognizing the privacy of the organization being investigated.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I think it was Paul who raised the question of the fact that if, it's not his word, it's my word, that it's a little dicey to make a determination that somebody is guilty before the final process has been exhausted.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Joyce DuBow – AARP Public Policy Institute – Associate Director
But I think it's clear that if an entity, an enterprise, is paying a fine that there has been some determination that there was guilt. And in that circumstance, I think that rather than suspend the payment, I think they should forego the payment that would have been made in that time period, because of the way that the payment schedule works. So that if they had qualified for a payment in 2012, that they shouldn't qualify for the payment during the time that they were in violation of the requirements. But that once they cure it, maybe in 2014, that they would qualify for whatever payment would apply in that year, which penalizes them. Because if you don't, if you simply suspend it, and then let them re-qualify, they can do it with impunity.

Gayle Harrell – Florida – Former State Legislator

I agree with you a hundred percent. I think the public will be outraged if they see anyone, an individual provider or a hospital or anyone who is taking Federal dollars while violating HIPAA regulations once it has of course been proven. There is a precedent as far as suspending payment or suspending even a licensor. In the state of Florida, a physician can have their license suspended once probable cause has been determined. So there are precedents out there for suspending payments in the case during the investigatory process. However—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You won't know when somebody's being investigated, that's my point.

Deven McGraw – Center for Democracy & Technology - Director
The public won't know, Dixie, it's an open question as to whether—

Gayle Harrell – Florida – Former State Legislator
The Feds will know.

Deven McGraw – Center for Democracy & Technology - Director
--OCR could trigger to CMS, here's someone that received a letter, that doesn't have to be made public necessarily and probably shouldn't quite frankly. I want to go back to Joyce's suggestion that we do this when in fact people are paying fines. Because it seemed as though, and again, I'm sort of taking the pulse of the group based on those who have been able, who have had a chance to speak, so I don't want to suggest that this is necessarily resolved, but it sounded like people were much more comfortable with the idea that when you've been found to be in violation and you're paying a fine, you ought not to be eligible for that year's payment in the year that you paid a fine.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
I'm looking back at the actual objectives and measure and I wonder if it may not apply any longer. The HIT policy committee's original recommendation, it did talk about being compliant with HIPAA. And in the NPRM though it says, let's say under objective, protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. You're implementing in EHR that has capabilities and the measure is conductor of user security risk analysis.

So one of the problems is, although we had intended it to be compliant with HIPAA, which is very reasonable and seems like an already bar that's there, it seems to have gotten limited to maintaining an EHR that has capabilities. Do you see what I am saying? So I'm not sure how the fine could be, I'm certainly very sympathetic to this direction.

Deven McGraw – Center for Democracy & Technology - Director
Yes, but Paul, so here's the thing, I think we're challenging CMSs decision, we're basically saying you should never have moved it and here's a way to implement it. This is the discussion that I got that I raised this with CMS and with ONC at the policy committee, because specifically with the idea of is this out of scope because it's not in the proposed rule.

And in fact, because it is mentioned in the proposed rule and they said why they rejected it, and then we got further information in the public policy committee meeting that said, "We were worried about what the trigger would be, we'd be interested in hearing from you if you think you can come up with an appropriate one." So I guess I'm challenging this notion that we're limited to the measure and the objective that are in the rule.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Okay.

Deven McGraw – Center for Democracy & Technology - Director
Because I don't think that's right, I mean, I don't think that's true.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think they actually invited comment about that.

Deven McGraw – Center for Democracy & Technology - Director
Yes, I agree, Dixie. So let me go back to what I think is the issue on the table, which is that with respect to, so let's deal with the civil actions where there are fines to be paid. Where somebody is paying a fine and I assume that we want to limit that still to the highest level of willful neglect, because there are penalty tiers for lesser offenses, like didn't know that there was a violation or a violation due to reasonable cause.

Gayle Harrell – Florida – Former State Legislator
I thought there were two top tiers.

Deven McGraw – Center for Democracy & Technology - Director
There's two top tiers and they're both due to willful neglect. One is willful neglect corrected and the highest is willful neglect uncorrected.

Gayle Harrell – Florida – Former State Legislator
In either case, they should not be paid.

Deven McGraw – Center for Democracy & Technology - Director
So you're putting on the table, Gayle, that for the top two penalty tiers, if they're being fined and they've gone through their appeal process and they have to pay and it's at one of those top two levels, they should be barred in the year that the fine is due?

Gayle Harrell – Florida – Former State Legislator
Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with her, I think—

Dave Wanser – NDIIC – Executive Director
The reality of it is that could be years between the time the offense occurs and the fine is levied. It gets complex from that standpoint in terms of something that might even play out after 2015 in terms of the actual fine being levied.

Deven McGraw – Center for Democracy & Technology - Director
Yes, I totally agree.

Gayle Harrell – Florida – Former State Legislator
In which case they then owe the money back.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Yes, they forfeit it.

Gayle Harrell – Florida – Former State Legislator
They forfeit it, they owe the money back, and believe me CMS has ways of getting that money back, believe me. They just don't pay you for next ...

Deven McGraw – Center for Democracy & Technology - Director
Like with certainly with which you attested to that, Gayle.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Yes, Gayle, I'm impressed with your level of experience with all of this stuff.

Mike DeCarlo - BCBS
I think that's right. I think you've got some criteria here in the meaningful use in which the measures will obviously not be forthcoming, so it will be apparent to CMS that the incentives should not be paid. But in this particular measure, if we do convince to go back and use the HIPAA compliance as a measure, this may become an overpayment or recoupment situation in which case CMS has come to the determination that we should not have paid you this money because you didn't meet this measure even though that determination is made many years later. So I think what you need is a clarification from CMS in this NPRM final rule that these incentive payments will be subject to overpayment recoupment's in out years if it is determined later that the measures were not met.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Mike DeCarlo - BCBS
When it's not apparent initially before the payment.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
I brought that up last meeting, so I agree with that. I think that the overpayment issue is going to be huge.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But if you think about, and I know the past isn't necessarily predictive in this case, but there would not be a whole lot of instances here.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Actually, you certified it, your EHR has these, you meet these criteria, and they come and they find that it doesn't, I think there's—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And it's not, yes, and the OCR completes a complete investigation and decides to penalize you, there are not going to be a whole lot of those.

Deven McGraw – Center for Democracy & Technology - Director
I think the reality is that we just don't know, but I want to get a sense of whether, it sounded like folks were onboard with where we were going here, and I guess I want to throw another wrinkle on the table, which is what do we do if people settle?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
My goodness.

Deven McGraw – Center for Democracy & Technology - Director
You thought you were out of the woods.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We thought we had it solved.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
It's those tricky lawyers I think.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
So they can settle for one on one side for the $200,000 and collected $2 million on the other hand.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Well that's actually, I sort of made it a joke, but it's actually real.

Joyce DuBow – AARP Public Policy Institute – Associate Director
It's a reality.

Gayle Harrell – Florida – Former State Legislator
It's a reality.

Joyce DuBow – AARP Public Policy Institute – Associate Director
And in fact, since there haven't been any penalties imposed and there only have been two settlements, this is a real issue.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Mike DeCarlo - BCBS
It still falls under the rule the agency has for determining recoupment of payments, overpayments, and if those were wiped off the table because of a settlement with the justice department or OIG, then it's effective for the incentives as it would be for payments for regular services.

Deven McGraw – Center for Democracy & Technology - Director
I see what you're saying, Mike. So often times in these settlements, the impetus for the company to agree to settle and to pay some money is that there's no finding of fault.

Mike DeCarlo - BCBS

Yes. They might not lose their participation capability.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
So we need some of the smart lawyers on this call to come up with a better way for us to—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Get out.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
--go get the bad guys.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Paul, I don't think we want to take on all the rules around payment recoupment and determination of ...

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Let's go back to first principles. We established this whole category as foundational, and this simple bar that already exists, we're not even adding anything, is that you need to be in compliance with HIPAA because it is so crucial to HIT adoption and effective use. I'm just arguing back for your case, Deven, we have to establish the HIPAA privacy and security as the low bar, the foundation, and have to find a way to give a ...

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Because we have found through our hearings that in fact even though it is, the law is in effect, it has a very low penetrance and we have to do something about it and this is what we're proposing to do.

Deven McGraw – Center for Democracy & Technology - Director
Yes, that's right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's exactly right, that's a very strong argument I think.

Deven McGraw – Center for Democracy & Technology - Director
A nice way to frame it, Paul.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Can I just ask one other question?

Deven McGraw – Center for Democracy & Technology - Director
Sure.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

This is outside the scope of privacy and security, but what happens if through a certification of other criteria, it is determined that somebody did not meet other criteria that they had certified to?

Deven McGraw – Center for Democracy & Technology - Director
You mean attested to?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
...

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
No, they can go out, because it's backed up by audits, so it's just like any other, Gayle, can tell you.

Gayle Harrell – Florida – Former State Legislator
... I can tell you. I know a lot of, no personal experience I will admit, no personal, I know a lot of situations though believe me.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm talking about for the meaningful use criteria, I'm not talking about the privacy and security stuff.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
... We're talking about the same thing.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I bet it's a quality measure and they don't meet up to the quality measures.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
But now if we're going to tie payments to a meaningful use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
But again, this goes back to the same question, if payments have been made for meeting other self-certification of other meaningful use criteria and it's determined that they haven't met those criteria after the fact, what's going to happen with regards to those payments, are they going to ask for them back?

Gayle Harrell – Florida – Former State Legislator
Sure.

Deven McGraw – Center for Democracy & Technology - Director
I think, I mean that's essentially Mike's point, Mike, if you don't mind me paraphrasing.

Mike DeCarlo - BCBS
No.

Deven McGraw – Center for Democracy & Technology - Director

But CMS already has the ability to do that, such as if you billed for a service that got paid for and then it turns out you didn't actually perform it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's fraud.

Mike DeCarlo - BCBS
...

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
How would their reaction to the failure of an organization to meet the security and privacy requirements differ then. If they would be the same, I guess, it wouldn't be suspended if they were made payments pursuit.

Mike DeCarlo - BCBS
It's a matter of authority I think, John. I mean, the authority to punish for failure to meet HIPAA is under OCR. We've confused things now, because we have payments for meaningful use incentives tied to payments for services and we want to take this HIPAA compliance as a measure for the incentives, so we're mixing the apples and oranges.

Joyce DuBow – AARP Public Policy Institute – Associate Director
But I think the difference is that HIPAA has a process that you have to go through. There's a define process to make a determination that there is in fact a violation. So all we're doing is waiting until that process has been exhausted. In the case of somebody who attests to something and it's fraudulent attestation, that entity is found out as soon as CMS conducts the audit. It's a different process.

Mike DeCarlo - BCBS
Right.

Joyce DuBow – AARP Public Policy Institute – Associate Director
But the end result is the same.

Mike DeCarlo - BCBS
But it's an OCR audit for HIPAA.

Joyce DuBow – AARP Public Policy Institute – Associate Director
Right, it's a different process.

Deven McGraw – Center for Democracy & Technology - Director
Okay, I think it's definitely different, I want to get us back onto what we're recommending. I realize that folks have some operational questions, but I want to make sure that we're onboard with what we're going to put forward to the policy committee, and then we've got a couple more things to cover, we're running out of time.

The one other piece that I threw up here, which was suggested by a workgroup member, is to make it clear that the meaningful use criteria regarding certain uses of healthcare information and data sharing don't override existing federal or state law that might set parameters around the access user disclosure of health information.

This was one that I was like, "Well doesn't everybody know that," but I don't think it hurts to underscore that for if there's a particular law that applies for example with respect to sharing of mental health data for care coordination, you have to meet that law, in addition to meeting whatever, the meaningful use criteria don't override that.

Joyce DuBow – AARP Public Policy Institute – Associate Director
I think that's obvious.

Deven McGraw – Center for Democracy & Technology - Director
Yes. I thought it was obvious too, but you just never know. So then the other piece to this that I laid on the table that we did have some discussion about is this issue of patient consent and whether in fact there is a standard sufficient in the certified EHR technology and whether it's, I happen to call it consent management or whether it's sort of bundled into what you need to prove for access control.

But I've laid out some bullet points here that are inevitably aimed at getting us to signal the importance of having the EHR technology have functionality that enables entities to appropriately manage consents when they're required. So this is not getting to the issue of when beyond what's already an existing law ought to be, where we ought to require patient consent, but acknowledging that in fact there are instances where patient consent or authorization is required. And that the technology ought to have a way of recognizing that through a technical standard or a functionality that is required through certification, and related to that is again this issue of data segmentation.

We were asked as a policy workgroup to focus our comments more on the notice of proposed rulemaking versus the rightness or the wrongness of standards in the IFR. But having said that, one of the responsibilities of the policy committee is to ask this, to make priorities for the standards committee to address. I know we've got Dixie right here on the phone who co-chairs the privacy and security workgroup of standards. I think the bottom line, there's a lot of language on these slides, but I think the bottom line of what we want to do is signal the importance of this for prompt action if it's not already well covered in the IFR, which to me I didn't think it was. And also to signal that we're going to be doing further work on this consent issue, which is really I hope by our next call actually to have a work plan for you all to review, that's the next task.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It seemed to me, the NPRM requirement about conducting the security risk assessment and make sure that you, if we get the language in about complying with HIPAA, already requires that access controlled capabilities would be in place for HIPAA covered entities. So the thing that's missing from my perspective is simply on the table to be in the IFR is a row that says access control and maybe just say comply with the HIPAA security access controlled requirements, which it has that functional standards sort of flavor that the other ones seem to share. But it is specific enough that it can be tested for in a certification environment.

Judy Sparrow – Office of the National Coordinator – Executive Director
Could you explain a little bit more what access control decisions mean in your opinion?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Who are you asking, me or—

Judy Sparrow – Office of the National Coordinator – Executive Director
I don't know, anybody who can help with that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Basically under HIPAA, the systems are required to control who, and there's a definition for access and it includes the access and the different uses and the disclosure of the data, so that when the system is running you ensure that the entity is accessing, using, or disclosing information out of the system are authorized to do so.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
I think Judy's question is a good one, because before I read the slide I hadn't understood that access control also included consent management.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It doesn't.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It doesn't. It's a tool for consent management.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And it doesn't include authentication either, and the second bullet here includes both of them. Verifying that a person or an entity is who they claim to be is authentication, determining whether they're authorized access to a particular resource that they've requested is access control.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
But you have to have authentication, wouldn't you agree, Dixie, in order to do the next step, which is the access control?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, right ...

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
And that if you do have privacy policy in your organization or you're trying to enforce a patient's consent, the way you do that in the system is you use your access control capability.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Right. So Dixie, I'm trying to understand your comment when I asked if access control includes consent management, you said it doesn't. So is what's written on this slide inaccurate or not quite right where it says access control processes consent management?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, there's several levels of consent management, and quite frankly I'd love to see those factored into the three stages too. There's consent management in kind of the ... perspective, which is really managing these signed documents that people have given their authorizations is really the right, because that's the only thing they have to sign, but they've given their authorization, so you've got a repository of authorizations. And that repository may not at all be connected to the access control capabilities of the system.

So the idea is ultimately overtime and we don't have good standards in this arena yet, they're still evolving, ultimately overtime you want to be able to have a machine interpret the metadata that's in that repository and translate it into access control rules that an access control system then enforces.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO

...

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I would just say that I think there are some actual implementations of ... enforced.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
There definitely are, but they're ...

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
...

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm talking about our 20% rule or of the industry uses, we don't have any like that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
... but elsewhere, they do use it and they do use it based on standards.

Deven McGraw – Center for Democracy & Technology - Director
Okay. So this is the one thing that I want to try not to delve to deeply into an issue that ought to quite frankly be resolved by the standards committee. But what I want to get a sense of is whether, it seemed to me that in fact the work wasn't necessarily all done in this area yet on standards, is that an accurate statement, Dixie, that there's more work that you guys need to do?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, we're reviewing the IFR now.

Deven McGraw – Center for Democracy & Technology - Director
Right, right. I mean that's what everybody's doing, but in terms of us as a workgroup recommending that the policy committee may get a priority for you all to—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, that's what we're waiting for, Deven, yes.

Deven McGraw – Center for Democracy & Technology - Director
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Absolutely, absolutely. I am eager, because the standards that we recommended for 2011 quite frankly have been, they've been based on HIPAA and HITSP work.

Deven McGraw – Center for Democracy & Technology - Director
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And so where I think, Dixie Baker speaking, that our priorities and for standards and privacy and security henceforth should be directly and strongly tied to the policy coming out of the policy committee, yes.

Deven McGraw – Center for Democracy & Technology - Director
Okay. So that sounds like it's within scope and maybe welcome at least by you personally for us to recommend that the policy committee make this a priority?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It's even in the law, yes, that's absolutely in the law, yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Well I'm confused is what's the priorities, is it access control, is it consent management, is it both?

Deven McGraw – Center for Democracy & Technology - Director
I think that I would phrase it rather than trying to dive into, which is the appropriate nomenclature? Would if we were to phrase it in terms of a technical standard or the requisite functionality to enable systems to manage consents or authorizations when they're required by law or by institutional policy.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Yes, but don't we, to pick up on what Dixie said, before we can give a priority and tell the standards committee that it's a priority, don't we have to do the policy work on some of these things, like segmentation first?

Deven McGraw – Center for Democracy & Technology - Director
Yes. I mean, undoubtedly we've got and want to take on this consent issue, but there already are consents required by law in certain instances, so what we would be doing as a group is building on that. And I guess it's theoretically possible that we might say, consent should never be needed, but I doubt it.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Well.

Deven McGraw – Center for Democracy & Technology - Director
And we wouldn't on our own accord have the ability to undo what's in state law even if we were inclined to be so bold.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Isn't the background on this and from the NTDHS studies that talked about they recommended that there may be sensitive types of information that should be afforded ...

Deven McGraw – Center for Democracy & Technology - Director
Well that's right, but we have taken that up, Kathleen, and so I think Paul's point is, and maybe it's better expressed as, that we're going to be taking this up and so to be beginning this work.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I'm agreeing with you, I was just saying the history of what I understood the history of the term data segmentation was something that has to be done prospectively, not ...

Deven McGraw – Center for Democracy & Technology - Director
Right. It is in the law, I think she's absolutely right about that.

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
Yes. I just think that we need to finish or have our own sense of policy on when consent is needed, what we're going to do with segmentation before we give a priority to the standards committee, because otherwise I'm just a little bit worried. The standards committee is going to do a ton of work.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Well isn't that—

Paul Tang – Palo Alto Medical Foundation – Internist, VP& CMIO
We're going to have like the tail wagging the dog, that work will determine of what we say on the policy ...

Mike DeCarlo - BCBS
I think what we have in the HIPAA law is that it gives each institution the capability to put in place its own institutional policies, which would give in a credence to segmentation and consent for that segmentation. What I'm saying is that trains left the station is the capability for segmentation to occur and for consent to control segmentation and the use of that information is out there and available.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
If there are areas—

Mike DeCarlo - BCBS
It's not a requirement, but it's available, and it's a requirement in some states.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I would agree, I think some of the issues that are areas in which consent policies have not been decided and I think that's what Paul's talking about, the data segmentation for example what can be allowed on the NHIN or in the HIE, places where there have not been definitive law on this. Is that right, Dixie?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree that that's, the HIE is certainly an area that we need to address some consent policies ranging all the way from opt in all, opt out, right down to the restricting access to particular data fields. But I think that when you look at, here's what I, I think you look at for example HIPAA, right now we know that—

Deven McGraw – Center for Democracy & Technology - Director
Dixie, I'm going to have to, we're like at 4:27, so we're going to have to get to closure here. I hate interrupting you, I know you're going to make a really good point, but we've just got to open up—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you, I'll make—

Deven McGraw – Center for Democracy & Technology - Director
--this call for public comment too.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'll make it offline.

Deven McGraw – Center for Democracy & Technology - Director
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's fine.

Deven McGraw – Center for Democracy & Technology - Director
So I think the general sense is that while we're not necessarily ready to say to the standards committee start working promptly on this. I think there's a way to word it to suggest that there be some concurrent

work, but that one piece of it shouldn't get out ahead of the other. And we ought to be in tandem because we're going to be dealing with whether there's new policy to be established here and in addition to needing to deal with the law we've already got on the books. Is that a fair statement however inaptly stated?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A roadmap, I like to think of it as a roadmap.

Deven McGraw – Center for Democracy & Technology - Director
Roadmap, that's a good way to put it. Alright, so let's go ahead and work to bring in the public, please.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great, operator, could you ask the public if anybody wishes to make a comment?

Deven McGraw – Center for Democracy & Technology - Director
And while we're doing that, here's what I will plan to do going forward, clean up these slides so that they appropriately encompass what we talked about on the call today. I thought it was a very good call. Thank you all for your patience. We had such a short amount of time and I think we made some real good progress, but I will re-circulate to you all and give you a chance to eyeball for me where you think I got it wrong. And if there's something major and we need to pull a call together to try to resolve it, we'll try to do that, hopefully that won't be the case. But I want to give you all another chance to look at this stuff before we sort of stamp the final on it and I'll get on that right away.

W
Thanks very much.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you.

Moderator
(Operator Instructions) We have no public comments.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great, thank you.

Deven McGraw – Center for Democracy & Technology - Director
Okay. Alright with that, wow, we ended on time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes, perfect.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Excellent, thank you, Deven.

W
Thank you.

M
Thank you, Deven, good meeting.

W
Thanks, Deven.

M
Thank you.

W
Goodbye.

M
Goodbye.